UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,342	04/12/2001	David John Craft	AUS920010088US1	3785

50675   7590   04/18/2007
IBM CORP. (CLG)
c/o CARDINAL LAW GROUP
1603 ORRINGTON AVENUE
SUITE 2000
EVANSTON, IL 60201

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>01 February 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1,2 and 4-40</u> is/are pending in the application.

    4a) Of the above claim(s) <u>1,2,4-9 and 40</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>10-39</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>2/2007</u>.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This office action is in response to applicant's remarks filed on 2/1/2007. Any

well known art statements made in the prior office action not adequately and/or

specifically traversed are taken as admittance of prior art as per MPEP 2144.03.

Claims 10-39 were examined.

Information Disclosure Statement

The IDS submitted by applicant on 2/1/2007 has been considered.

Response to Arguments

Applicant's arguments filed on 2/1/2007 have been fully considered but they are

not persuasive.

With respect to the 101 rejection of claims 13-15, 21-22, 27-28, and 34-36,

applicant essentially states that 112, sixth paragraph was invoked and the claims must

be interpreted in light of the structure disclosed in the specification and pointed to at

least Figures 1A, 1B, and 2 of the present application as disclosing statutory subject

matter for the means recited in the claims. The examiner respectfully points out that

Figures 1A and 1B are labeled as prior art, thus are not structures related to the claimed

invention. Further, applicant's specification states that the invention may be

implemented on a variety of hardware platforms **and a variety of software**

environments (see last paragraph on page 12 of specification). Thus, the examiner did

interpret the claims with respect to the structures disclosed in the specification as

required by 112, sixth paragraph. It is applicant's specification which discloses that the

structure claimed may either include hardware or be implemented as software alone.

Further evidence that the claimed means can be implemented as software alone can be

seen in claim 16, where the claimed means are recited as instructions, i.e. software per

se. Thus, because at least one of the embodiments disclosed by applicant's

specification shows the claimed means as being software per se, the 101 rejections of

the claims are maintained.

With respect to claims 10, 13, and 16, applicant argues that Aoki does not teach

a client public key stored exclusively outside the client. Applicant states that Aoki

requires that an individual public key be present at the client for at least part of the

certification method, thus storing the individual public key in the client. The examiner

respectfully disagrees. It is true that a public/private key pair is created in the client

taught by Aoki (col 8, lines 39-54). However, there is nothing disclosed by Aoki which

suggests that the public key is saved in the client after the creation of the public key.

Rather, the public key is sent to the server after creation (col 8, lines 46-49). Figure 1,

item 200 and column 7, lines 46-49 shows what is retained/stored in the memory of the

client. The client's individual private key of the created public/private key pair is shown

to be stored in the client. The client's public key itself is not shown to be stored in the

client despite both the public key and the private key having been created in the client.

At the very least, this would suggest to one of ordinary skill in the art that the public key

is not stored in the client after creation, but rather is stored exclusively outside the client.

Applicant argues also for claims 10, 13, and 16 that Arnold lacks motivation to

modify its teachings to embed a client's private key in read-only memory. The examiner

respectfully disagrees. Motivation was given in the office action. The first motivation

given was that utilizing read-only memory to store keys (this includes the client's private

key) would allow key information to be retained even if the device containing the

memory were to lose power. The second motivation given came from Arnold himself

(col 4, lines 36-40): "use of read-only memory to store the keys prevents tampering with

information stored in the memory, thus providing better security".

        Applicant argues for claims 10, 13, and 16 that there is no motivation to combine

Arnold and Aoki. Applicant states that Arnold is directed towards establishing a secure

cryptographic network among operational units in a system while Aoki is directed

towards establishing a certification system for an entire enterprise. Thus there is no

need for the secure cryptographic network of Arnold on top of the certification system of

Aoki since the certification system is already secure. The examiner respectfully

disagrees. Certification as taught by Aoki provides for authentication, but does not

necessarily provide for secure communication. For instance, if a first party offers a

certified identification card to a second party, the first party's identity would then be

proven/authenticated to the second party. However, any conversation held between the

two parties is not necessarily secure from eavesdropping. Certification and secure

communication are two different security concerns that are known in the networking art.

Thus, because Arnold can provide for secure communication, while Aoki provides for

certification, there is motivation to combine the two references since each reference

addresses different security concerns.

Applicant's arguments for the other independent claims of the present application

are the same as what was argued for claims 10, 13, and 16 and are traversed for the

same reasons. Applicant's argument for the dependent claims is that they are allowable

due to dependency. However, because the arguments for the independent claims are

traversed, the dependent claims are also not allowable.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the
conditions and requirements of this title.

Claims 13-15, 21-22, 27-28, and 34-36 are rejected under 35 U.S.C. 101

because the claimed invention is directed to non-statutory subject matter.

Using claim 13 as an example, claim 13 is a claim to an apparatus comprising

means for performing various steps of a method (the method of claim 10). As

evidenced by claim 16, the means being claimed are instructions, i.e. software. As

such, claim 13 is directed towards an apparatus that is software per se, which is not

statutory. Claims 14-15, 21-22, 27-28, and 34-36 are also directed towards apparatuses

that are software per se as the means recited in the claims are implemented as

instructions, i.e. software. The claimed apparatuses must comprise at least one

component that is hardware to overcome the 101 rejections for the claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10, 13, and 16 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530).

Claims 10, 13, and 16:

As per claim 10, Arnold discloses the following limitations were will known in the

art at the time applicant's invention was made:

1. Generating a client message at the client (col 2, lines 9-24).

2. Retrieving an embedded server public key from a memory structure in an article

   of manufacture (col 2, lines 9-24).

3. Encrypting the client message with the embedded server public key (col 2, lines

   9-24).

4. Sending the client message to the server (col 2, lines 9-24).

Arnold does not explicitly disclose that in the prior art he discusses, the memory

structure is read-only memory. Arnold also does not explicitly disclose the article of

manufacture is in the client, the read-only memory structure having an embedded client

private key, the embedded server public key and the embedded client private key not

being related by a public/private key pair relationship, the embedded client private key

being associated with a client public key stored exclusively outside the client.

However, Arnold discloses read-only memory being used to store keys (col 4, lines 14-17). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the prior art teachings disclosed by Arnold so that the memory structure used to store keys was read-only memory structure. One skilled would have been motivated to do so because one skilled would appreciate that utilizing read-only memory to store keys would allow key information to be retained even if the device containing the memory were to lose power. One skilled would also be motivated to do so because use of read-only memory to store the keys prevents tampering with information stored in the memory, thus providing better security (Arnold: col 4, lines 36-40).

Further, Aoki discloses the article of manufacture is in the client, the memory structure having an embedded client private key, the embedded server public key and the embedded client key not being related by a public private key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client (Fig 1, item 200). Note that in the figure cited, the client has stored in memory the client's private key, i.e. individual private key, and a server's public key, but no client public key. As the client does not store the client's public key, the client's public key is stored exclusively outside the client. The private key of the client and the server's public key are not related by a public/private key pair relationship as they do not have an inverse relationship with one-another, i.e. plaintext encrypted by one cannot be decrypted by the other.

At the time applicant's invention was made, it would have been obvious to one

skilled in the art to modify the client/server system disclosed by Aoki to use the secure

communication techniques taught by Arnold (what he reveals was known in the prior art

as well as what his own invention uses) such that a method as recited in claim 10 is

implemented. One skilled would have been motivated to do so because it would allow

Aoki's network system to establish a private and secure link between the clients and

server of his invention for secure communication (Arnold: col 2, lines 23-24 and 43-44).

Claim 13 is directed towards an apparatus comprising means for implementing

the method of claim 10 while claim 16 is directed towards a computer program product

comprising instructions for implementing the method of claim 16. As such, claims 13

and 16 are rejected for substantially the same reasons given for claim 10.

Claims 11, 14, and 17 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) and further in

view of Sandhu et al (US 2002,0078344).

Claims 11, 14, and 17:

As per claims 11, 14, and 17, the combination of Arnold and Aoki discloses

embedded client private key in a memory structure in an article of manufacture in the

client (Aoki: Fig 1, item 200); the memory structure being read-only memory (Arnold: col

4, lines 14-17); and retrieving the client private key from the client's memory (Arnold: col

2, lines 25-41).

Arnold and Aoki do not explicitly disclose retrieving client authentication data; encrypting the client authentication data with the embedded client private key; and storing the encrypted client authentication data in the client message. However, these limitations are disclosed by Sandhu (paragraph 28).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Arnold and Aoki's combination invention according to the limitations recited in claims 11, 14, and 17 in light of Sandhu's teachings. One skilled would have been motivated to do so because it would provide client-side authentication (paragraph 28), thus making communication between the client and server more secure. Note that Arnold discusses authentication being desired objective for secure communication since before the time of his invention (col 2, lines 43-48).

Claims 12, 15, 18, 25, 27, 29, 26, 28, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold (US 5,787,172) in view of Aoki (US 6,745,530) and further in view of Sandhu et al (US 2002,0078344) and further in view of Davis (US 5,970,147).

Claims 12, 15, and 18:

As per claims 12, 15, and 18, Arnold, Aoki, and Sandhu do not explicitly disclose retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and storing a copy of the embedded client serial

number in the client message. However, these limitations are disclosed by Davis (col 4, lines 26-39; col 5, lines 58-62; and col 6,lines 27-29).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify the combination invention of Arnold, Aoki, and Sandhu according to the limitations recited in claims 12, 15, and 18. One skilled would have been motivated to do so because the client sending the serial number to the server alone with its message would allow the server to index various clients' public keys to the client's serial number, thus providing for a way for the server to look up the client key needed to authenticate the client's message.

Claims 25, 27, and 29:

As per claims 25, 27, and 29, the limitations recited therein are directed towards the server receiving and processing the message sent using the method, apparatus, and computer program product of claims 12, 15, and 18 respectively. One skilled would appreciate that a message sent by a client according to the limitations recited in claims 12, 15, and 18 would be processed by the server according to the limitations recited in claims 25, 27, and 29, thus the rejections for claims 25, 27, and 29 flow from the rejections of claims 12, 15, and 18 respectively.

Claims 26, 28, and 30:

As per claims 26, 28, and 30, the limitations recited therein are directed towards the server processing the authentication data sent by the client using the method, apparatus, and computer program product of claims 11, 14, and 17 respectively. One skilled would appreciate that a message sent by a client according to the limitations

recited in claims 11, 14, and 17 would be processed by the server according to the

limitations recited in claims 26, 28, and 30, thus the rejections for claims 26, 28, and 30

flow from the rejections of claims 11, 14, and 17 respectively.

Claims 19, 21, 23, 31, 34, and 37 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Arnold (US 5,787,172) in view of official notice by the examiner and

further in view of Aoki (US 6,745,530).

Claims 19, 21, and 23:

As per claim 19, Arnold discloses the following limitations were will known in the

art at the time applicant's invention was made:

1. Generating a server message at the server (col 2, lines 9-24).

2. Retrieving a client's public key (col 2, lines 9-24).

3. Encrypting the server message with the client's public key (col 2, lines 9-24).

4. Sending the server message to the client (col 2, lines 9-24).

Note that the cited portion of Arnold discloses communication between two

elements A and B. One skilled should appreciate that both A and B can be either a

client and/or server.

Arnold does not explicitly disclose that the prior art he discusses teach the

following limitations:

1. Retrieving information that was requested by the client.

2. Storing the retrieved information in the server message.

3. Wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client.

However, that Arnold also discloses read-only memory being used to store keys (col 4, lines 14-17). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify the prior art teachings disclosed by Arnold so that the memory structure used to store keys was read-only memory structure. One skilled would have been motivated to do so for the same reasons given in the rejection of claims 10, 13, and 16.

Further, the examiner take official notice that retrieving information that was requested by the client and storing the retrieved information in the server message was well known in the art at the time applicant's invention was made. Note that these limitations were also discussed as being well known in the art at the time applicant's invention was made in the prior office action.

Further, Aoki disclose wherein the client public key corresponds to an embedded client private key in a memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client (Fig 1, item 200).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to combine the above teachings to arrive at an invention as

recited in claims 19, 21, and 23. One skilled would have been motivated to incorporate

Arnold's teachings with Aoki's client/server system for the same reasons discussed

above in claims 10, 13, and 16. One skilled would have been motivated to incorporate

the teachings the examiner took official notice on because these teachings describe

typical client-server relationship, i.e. a client requests information being "served" by the

server, the server retrieves the requested information, and sends it to the client via a

server message provided that the client is authorized to receive the information.

Claims 31, 34, and 37:

As per claims 31, 34, and 37, the limitations recited therein are directed towards

the client receiving and processing the message sent by the server using the method,

apparatus, and computer program product of claims 19, 21, and 23 respectively. One

skilled would appreciate that a response message sent by a server according to the

limitations recited in claims 19, 21, and 23 would be processed by the client according

to the limitations recited in claims 25, 27, and 29, thus the rejections for claims 31, 34,

and 37 flow from the rejections of claims 19, 21, and 23 respectively.

Claims 20, 22, 24, 32, 35, 38, 33, 36, and 39 are rejected under 35 U.S.C. 103(a)

as being unpatentable over Arnold (US 5,787,172) in view of official notice by the

examiner and further in view of Aoki (US 6,745,530) and further in view of Sandhu et al

(US 2002,0078344).

Claims 20, 22, and 24:

As per claims 20, 22, and 24, Arnold discloses retrieving a server private key (Arnold: col 2, lines 25-41).

Arnold does not explicitly disclose retrieving server authentication data; encrypting the server authentication data with the server private key; and storing the encrypted server authentication data in the server message. However, these limitations are disclosed by Sandhu (paragraph 27).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify the Arnold's invention according to the limitations recited in claims 20, 22, and 24. One skilled would have been motivated to do so because it would provide server-side authentication (paragraph 27), which would make communication between the client and server more secure.

Claims 32, 35, and 38:

As per claims 32, 35, and 38, the limitations recited therein are directed towards the client receiving and processing the message sent by the server using the method, apparatus, and computer program product of claims 20, 22, and 24 respectively. One skilled would appreciate that a response message sent by a server according to the limitations recited in claims 20, 22, and 24 would be processed by the client according to the limitations recited in claims 32, 35, and 38, thus the rejections for claims 32, 35, and 38 flow from the rejections of claims 20, 22, and 24 respectively.

Claims 33, 36, and 39:

As per claims 33, 36, and 39, Arnold does not explicitly disclose retrieving requested information form the server message; and in response to a determination that

the decrypted authentication data was verified, processing the requested data.

However, the examiner take official notice that the limitations were well known in the art

at the time applicant's invention was made. Note that these limitations were also

discussed as being well known in the art at the time applicant's invention was made in

the prior office action. These limitations describe a typical client-sever relationship. A

client typically requests information from a sever, the server receives the request, and if

the client is authorized to receive the information the server sends the information to the

client who receives the requested information via the server's reply message. The

client typically only processes the information sent by the server if the decrypted

authentication data was verified for security purposes.

At the time applicant's invention was made, it would have been obvious to one

skilled in the art to further modify Arnold's invention according to the limitations recited

in claims 33, 36, and 39. One skilled would have been motivated to do so because the

limitations further recited in claims 33, 36, and 39 describe a typical client-server

relationship.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
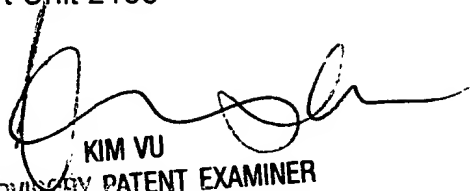
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich

PP

Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100